Information & Security: An International Journal

Atalay & Sanci, vol.32, 2015 http://dx.doi.org/10.11610/isij.3203

CYBERTERRORISM AND TURKEY'S COUNTER-CYBERTERRORISM EFFORTS

Ata ATALAY and Gurur SANCI

Abstract: Technological innovations leading to the industrial revolution in the 19th century have proceeded in an accelerated manner to lead to an information revolution in the 21st century. In addition to warfare in land, sea and air domains, "space" has emerged as a new field of operation. Further technological innovations have yet again set up another domain called "cyberspace," dominated by information technologies with the capability to change the course of war on land, sea, air and/or space. Besides, organised crime and terrorist organisations, following the progress in cyberspace technologies, have increased their profits and developed new types of crime using new types of weapons. Attacks in the cyber domain evolve so rapidly that legal arrangements cannot cope with meeting security requirements and need to be frequently updated. On the other hand, new threats, such as "cyberterrorism," necessitate wide-scope interpretation of the norms in international law. Turkey has taken several counter-cyberterrorism precautions. The establishment of the Cyber-security Council, the adoption of the National Cybersecurity Strategy and of the 2013-2014 Action Plan are major steps in this regard. The rapid development in communication technologies has removed the national boundaries, increasing and gradually deepening the interaction between countries. Therefore, in order to strengthen cybersecurity efforts, it is necessary to further international cooperation as well as the cooperation between local public authorities and the private sector.

Keywords: cyberpace, cyberwar, cyberterrorism, counter-cyberterrorism, cyberattack, cybersecurity, Turkey, 2013-2014 Action Plan.

Introduction

Technological innovations leading to the industrial revolution in the 19th century have proceeded in an accelerated manner, leading to the information (or digital) revolution of the 21st century. In our century, traditional concepts such as "time," "space," "transformation," "language," etc., are being replaced with new terms – "24-hour day," "cyberspace," "speed of light," "pictogram," "digital content," etc.[1]

In addition to warfare taking place on land, sea and air, "space" emerged as a new domain of operation owing to developments in technology. Innovations have yet

again set up another domain called "cyberspace," dominated by information technologies with the capability to change the course of war on land, sea, air and/or space.

Internet, the leading factor in the information revolution, was first developed and used for military purposes in the 1960s. The Internet technology is improving since then. According to the report of the United Nations International Telecommunication Union (ITU), the number of Internet users will reach 3.2 billion by the end of 2015.[2]

With the spread of the Internet all over the world in the 1990s, the concept of "space-time" continuum lost its original meaning; electronic communication through computers replaced the time-consuming information transfer on paper, thus the process of domestic and international communication became so simplified that now pushing a button is enough to transfer information. Besides data transfer, computers also provide greater capacity for both storing and processing information. Yet this fast progress in technology has brought some particular problems to the world's agenda, such as attacks on private and public electronic information networks.

Organised crime and terrorist organisations, utilising the progress in cyberspace technologies, increased their profits on the one hand, and developed new types of crime using new types of weapons, on the other. Their activities generally transcend national boundaries ending up with the emergence of transnational crime. Organised crime and terrorist organisations, benefitting from these new types of crime, attract the public attention due to the resulting public losses and the difficulties in catching and punishing their members. It is observed that terrorist organisations generally target easily accessible and vulnerable points such as airports, hospitals and energy transmission stations. Walter Laqueur, in an article in the journal *Foreign Affairs*, claimed that "If the new terrorism directs its energies toward information warfare, its destructive power will be exponentially greater than any it wielded in the past – greater even than it would be with biological and chemical weapons."[3]

In today's world of rapid transformation, organised crime and terrorist organisations often exploit new opportunities faster and more effectively than governments do and, due to the easy access to information, can easily convert information into intelligence. Their capacity to benefit from this fast and continuous global transformation constitutes a severe threat to international peace and national security of states.

Cyberterrorism and Cyberwar

The term "cyberterrorism" was coined in the 1980s by Barry Collin, a senior research fellow at the Institute for Security and Intelligence (ISI)[4] in California. Collin defined cyberterrorism as "the intentional abuse of a digital information system, network, or component toward an end that supports or facilitates a terrorist campaign or action."[5]

A widely accepted definition was provided in 1998 by Mark M. Pollitt, an FBI Special Agent. He described cyberterrorism as "premeditated, politically motivated attack against information, computer systems, computer programmes and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."[6]

According to Nihat Ali Özcan, a leading Turkish scholar on terrorism, cyberterrorism is "a set of personally and politically motivated intentional acts and activities, aiming to devastate national balance and interests by exploiting electronic media, computer programmes or other electronic communication types."[7]

Mesut Hakkı Caşın, a prominent Turkish scholar on international terrorism, argues that a crime committed in cyberspace is cyberterrorism in case the action:

- pursues racist, ideological, religious or political aims;
- is perpetrated through a computer or a computer system;
- creates fear and horror in target society;
- causes a physical damage or targets a facility vital for immediate human survival.[8]

In summary, "cyberterrorism" may simply be defined as "acts of organised crime and terrorist organisations through exploiting computers and computer systems."

Cyberwar is slightly different from cyberterrorism with respect to the actors. Richard Clarke, Special Advisor to former President George W. Bush on cybersecurity, whose definition has been widely used in international literature, describes cyberwar as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[9] Clarke identifies some of the outstanding characteristics of cyberwar:

- "Cyberwar skips the battlefield": Systems, people rely on (from banks to air defence radars) and accessible from cyberspace, can be quickly taken over or knocked out without first defeating a country's traditional defences.
- "Cyberwar is real": Attackers do not want to reveal their more sophisticated capabilities and what nations are capable of doing in a cyberwar could devastate a modern nation.

Cyberspace Weapons

In a century in which our social and financial lives have been transferred to the cybersphere, organised crime and terrorist organisations or hostile nation-states could easily and adversely affect our lives in various ways, including damaging banking and financial systems,[10] paralysing power systems indefinitely, disrupting emergency ser-

vices, hampering with take-offs or arranging plane crashes, manipulating traffic lights to create accidents to lead to urban chaos, and starting fires and explosions in refineries and nuclear plants.

For a terrorist or a hostile nation to be able to cause such harm, there are some cyber weapons, including viruses, worms, trojans, DoS attacks, unsolicited electronic messages, keystroke logging programmes and phishing, etc. These are shortly defined as follows:

- *Viruses* refer to a sort of malware programme spreading via infecting other files.
- *Worms* are designed to replicate themselves in other devices and can spread quickly.
- *Trojans* are computer software infecting the system generally through free software which appears to have a useful function.
- *Unsolicited Electronic Messages (Spam)* are e-mails which are seemingly sent for advertisement or propagation purposes but infect computers with malware.
- *Keystroke Logging Programmes (Key loggers)* stealthily record the keys struck on a keyboard and send these recorded actions to designated addresses.
- *Phishing* is an illegal attempt to acquire personal information of users through designing fake websites that look just like their legitimate counterparts.

Economic Cybercrime

This study focuses on cyberterrorism and cyberwar, which are politically motivated and which bring about consequences that influence an audience beyond the immediate victim. Cybercrime, excluded by the study, involves "committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy, etc.,"[11] that is, activities with no political motivation. Yet, for instance, if terrorists use computers as a facilitator of their activities, whether for propaganda, recruitment, data mining, communication or other purposes, then we cannot say that it is cyberterrorism.[12] These activities should be included in cybercrime.

The possibility of using cybercriminal acts to fund terrorism has gained strength in recent years. Hence a look will be given below at cybercrime, concentrating on the economic sphere, namely economic cybercrime, with reference to statistical data.

According to a report of the United Nations Office on Drugs and Crime, the most profitable cybercrime is "identity theft" which leads to a global loss of US$ 1 billion annually.[13] The table below indicates which items can be stolen online for the purpose of economic gain.[14]

Depending on a study conducted in 2013 by Ponemon Institute, Figure 1 presents the average cost of cybercrime estimated for six countries with a total benchmark sample of 234 organisations. The study reveals the high increase in cost of cybercrime over a short time period. When compared with the amount in 2010, that cost of cybercrimes in 2013 has increased by approximately 75% in just four years. Depending on the data from the benchmark sample of 60 US organisations which reported their cost of cybercrimes over four consecutive weeks, the mean value of the annualised total cost of cybercrime was estimated to be approximately $11,6 million (compared to $6,5 million in 2010).[15]

Table 1: Breakdown of goods available for sale on underground economy servers (Source: Symantec Corporation, 2007).

Rank	Item	Percentage	Range of Prices
1	Credit Card Numbers	22%	$0.50 - $5
2	Bank Accounts	21%	$30 - $400
3	Email Passwords	8%	$1 - $350
4	Mailers	8%	$8 - $10
5	Email Addresses	6%	$2/MB - $4/MB
6	Proxies	6%	$0.50 - $3
7	Full Identity	6%	$10 - $150
8	Scams	6%	$10 / week
9	Social Security Numbers	3%	$5 - $7
10	Compromised UNIX® Shells	2%	$2 - $10

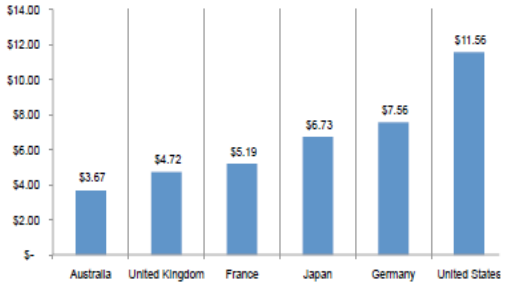

Figure 1. Total cost of cyber crime in six countries (Cost expressed in million US dollars, n = 234 separate companies; Source: Ponemon Institute, 2013).

Figure 2 below illustrates that although the technical knowledge of the average attacker has been declining, the sophistication of Internet attacks has increased over time. Consequently, while organising cyberattacks is gradually becoming easier, cyberattacks are increasing in number.[16]

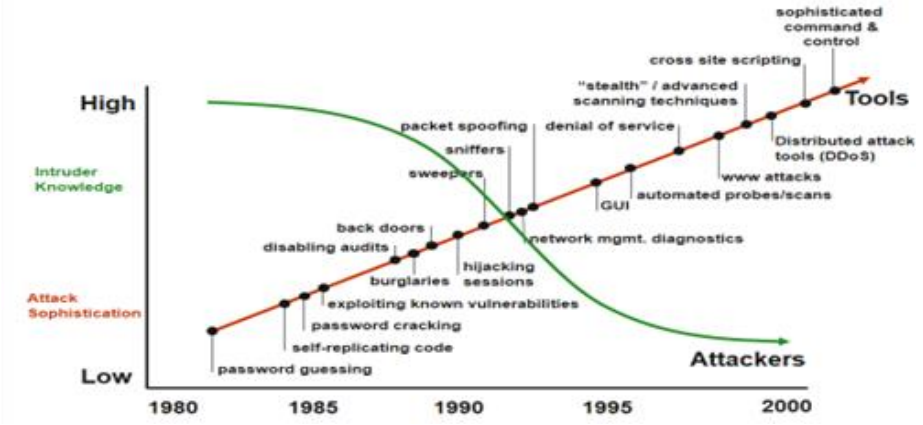

Figure 2: Attack Sophistication vs. Intruder Technical Knowledge (Source: Carnegie Mellon University Software Engineering Institute, 2002).

Traditional Terrorism vs. Cyberterrorism

When compared to traditional terrorism, cyberterrorism has some tactical advantages for the attacker. Firstly, traditional terrorist groups are well aware that they risk their lives while planning their activities. A suicide attack or an attack targeting security forces would most probably result in loss of their lives. In cyberterrorism, on the contrary, a member of a terrorist organisation with only an Internet-connected computer would be able to create a greater impact. A cyberattack against a finance system

would be more devastating and sensational than a suicide attack, and the attacker, unlike a traditional terrorist, would not be under life risk.

Secondly, even though terrorist organisations' propaganda reaches the masses, the activity itself is in a way "local."[17] In traditional terrorism, a terrorist may blow up a public building and kill almost everyone inside it, yet this act is limited only to the building and the people inside it. Contrariwise, a terrorist engaging in cyberterrorism can easily expand the physical space of action by just using a "mouse," collapse thousands of public organisations' websites simultaneously at the speed of light, thus damaging computer-controlled water and electric power distribution systems and affecting the lives of thousands of people, leading to chaos.[18]

Third, while traditional terrorist organisations generally exploit their own members in their actions, with the emergence of cyberterrorist organisations, there has also emerged the possibility of using "subcontractors." In this regard, security forces, used to follow the activities of traditional terrorist organisations, now face difficulties in proactive intelligence gathering to counter cyberterrorist activities since the individual who performs cyberattack is not a member of the organisation.

Fourth, although it is normally expected that a traditional terrorist attack evokes emotional reactions from society, it is highly unlikely that a cyberterrorist attack arouses any emotional reaction from society since in most cases nobody dies or gets injured during the attack (at least at the very moment of action).

Fifth, traditional terrorists, via the activities they carry out, send a message to a political regime or society. In the way to this goal, violence and damage are their basic tools. However, with the shift to cyberterrorism, violence is becoming a goal rather than a tool.

Sixth, in today's world with the developments in technology, "space" and "time" are not anymore conceived as impediments and terrorist organisations are able to communicate with their members through encrypted channels. Terrorist organisations materialising terrorist activities by keeping in touch through encrypted messages, can exploit Internet capabilities also to spread political and ideological propaganda. For instance, "FARC" in Colombia and "Shining Path" in Peru use the Internet intensively. On the Internet, one can also reach some resources such as "The Terrorist's Handbook" or "The Anarchist Cookbook" which contain detailed instructions on the process of creating and detonating a wide variety of explosives.[19]

Seventh, it is relatively easy to determine the source of attack in traditional terrorism; in cyberterrorism, however, it is extremely hard or almost impossible to find out where the action originates from.

Eighth; while in traditional terrorism physical effects allow easier damage assessment, in cyberterrorism, it is extremely difficult, and in most cases impossible, to assess the magnitude of damage.

Interaction between Cyberoffense, Cyberdependence and Cyberdefence

In international literature, mobilisation and war-making capacity of a nation is directly related to the number of its soldiers, the level of their training, the sophisticated technological weapon systems in possession, the ability to continue the production of these weapon systems both in peace and war times and other national power elements (economy, population, technological development, geography). In the sphere called "cyberspace," on the other hand, the cyberwar capacity of a nation can be measured depending on its active cyberwar elements, its cyberwar prevention and research teams, its computer incident response teams, its applicable cyberwar doctrine, the extent of government's participation in academic programmes in cybersecurity, its level of utilisation of information technologies and the extent of the availability of government funds for technology innovation programmes.

According to Richard Clarke, cyberwarfare strength does not only mean the ability to attack other nations. "Defence" and "dependence" are the two other factors that also need to be assessed in measuring cyberwar strength. The table below[20] illustrates the interaction between several countries for each of these three factors: cyberoffense, cyberdependence and cyberdefence.

To the extent critical infrastructures of a nation are dependent upon networked systems and have no real backup, the nation's cyberwarfare capability would be low. From the information in the table, we see that the US has the lowest score on the "cyberdependence" ranking,[21] since it is the most wired nation among those listed in the table. China has a high score for "cyberdefence," because it can limit cyberspace

Table 2: Overall Cyberwar Strength (Source: Clarke and Knake, 75).

Nation	Cyberoffense	Cyberdependence	Cyberdefence	Total
USA	8	2	1	11
Russia	7	5	4	16
China	5	4	6	15
Iran	4	5	3	12
N. Korea	2	9	7	18

utilisation when needed by disconnecting nonessential users. Having so few systems dependent upon cyberspace, North Korea has the highest score on the overall cyberwar strength ranking. In case of a major cyberwar attack, North Korea can easily and effectively sever its limited connection to cyberspace.

Countries' Cyberwar Capabilities and Strategies

In another study, which was conducted by Verisign Corporation, nation-states were broken down into four major groups depending on the level of their cyberwar capabilities as shown in the table below.[22]

Table 3: Cyberwarfare Capabilities of Selected Nation States (Source: Çiftçi, 25).

Group	Nation-States	Characteristics	Organizational Scope	Capabilities
First Group	USA China Russia	They are capable of setting international policy on cybersecurity and allocate to this undertaking the greatest amount of resources, including manpower	They have lots of well-defined and specialized intelligence and military organizations	Integrating the cyberspace into the conventional sphere, they are capable of carrying out comprehensive and continuous offensive and defensive activities.
Second Group	England France Israel	They follow the countries in the first group, yet have less resources and infrastructure	They have lots of well-defined and specialized intelligence and military organizations; however, they have allocated less resources for cyber	They are capable of conducting continuous and complex offensive and defensive activities against other countries, yet limited in scope and less in number of countries
Third Group	Turkey Taiwan N. Korea	They allocate a good deal of resources to the cyber sphere; however, they follow the first group of countries in many aspects	Although they have several well-defined organizations, these organizations need to be institutionalized	They are capable of conducting continuous and comprehensive defensive activities, yet their offensive capabilities are weak
Fourth Group	Iran Pakistan Australia	They allocate limited resources to cybersecurity and cyberdefence	They have only a few organizations, which need to be improved	They conduct strong but insufficient defensive and limited offensive activities. They try to maintain their domestic resources

The USA, which is in the first group in the above-mentioned research by Verisign Corporation, has four cybersecurity organisations operating in coordinated manner. These are the U.S Cyber Command, the National Security Agency, the Department of Homeland Security and FBI. Out of the four organisations, the Cyber Command was officially launched in 2010 with responsibilities for maintaining the safety of networks, thus protecting the USA against cyberattacks. It has 900 personnel consisting of military and civilian experts, with plans to increase this number. The Command has both offensive and defensive capabilities and shall integrate these capabilities into the operational plans of combatant commands and help the Department of Homeland Security in protecting critical infrastructures. Within the Command, 13 teams have offensive capability and 27 teams have both offensive and defensive capabilities.

China, on the other hand, trying to further nuclear and space studies, established its cyberwar unit called "Blue Army" in 2011. China has four agencies—two of them under the People's Liberation (PLA) Army General Staff Headquarters—responsible for the cyber sphere. For instance, the 3rd Department of the PLA General Staff Headquarters, allegedly staffed by more than 130 thousand people, gathers and analyses foreign signals intelligence and maintains the safety of Chinese communications networks.[23] It is claimed that Chinese hackers, through exploiting software deficiencies as yet unfamiliar to the world, organise cyberattacks and capture commercial and military information.

In the United Kingdom, the two main institutions responsible for the cyber domain were envisaged in the first Cybersecurity Strategy of the United Kingdom of June 2009.[24] Accordingly, the Office of Cybersecurity, responsible for coordinating cybersecurity programmes run by the UK government, was established in September 2009 and became the Office of Cybersecurity and Information Assurance (OCSIA) in 2010;[25] and the Cybersecurity Operations Centre (CSOC), which is "responsible for providing analysis and overarching situational awareness of cyber threats," was formed in 2009.[26] These institutions are assisted by some other agencies including the UK Government Communications Headquarters, the Centre for the Protection of National Infrastructure, the Department for Business, Innovation and Skills, the Computer Emergency Response Teams (CERTs) and the Police Central e-Crime Unit. The National Security Strategy of October 2010 rated cyberattacks as a "Tier 1" threat.[27] Accordingly, the Strategic Defence and Security Review of October 2010[28] envisaged a four-year transformative National Cybersecurity Programme (NCSP) with a budget of £650 million to mitigate the risks against 21st-century communications. The UK Government launched the Programme in 2011, to be updated in September 2014 and extended until March 2016 with a renewed budget of £860 million.[29]

France's 2008 White Paper on Defence and National Security[30] covered cybersecurity issues. The document envisioned the establishment of a new agency for coordi-

nation of cyberdefence under the purview of the General Secretariat for Defence and National Security (SGDSN) and the establishment of an offensive cyberwar capability, one part to be placed under the Joint Staff and the other part to be developed within specialised services. Following the recommendations in the 2008 White Paper, the French Network and Information Security Agency was set up in 2009 responsible, *inter alia*, to support the production of France's own safety products and services for public and private actors. France's 2013 White Paper on Defence and National Security reinforces the importance of the cyber domain as regards national security. It reaffirms that the possibility of a major cyberattack on national information systems constitutes an extremely serious threat to France. Therefore, it envisages the development of "an approach based on a cyberdefence organisation closely integrated with the armed forces, made up of defensive and offensive capacities." The 2013 White Paper, furthermore, underlines that "the operational organization of the armed forces will incorporate an operational cyberdefence platform, consistent with the operational organization and structure of the French armed forces and adapted to the specific characteristics of this sphere of combat."[31]

Cyberterrorism in the Context of International Law

The difficulty of defining "terror," "terrorist" and "terrorist action" in the context of traditional terrorism is also reflected in the domain of cyberterrorism, hence yet we do not have an explicit, agreed upon definition for "cyberterrorism" in the international law.

Cyberterrorism and the UN

The principles of "non-intervention in domestic affairs by the United Nations," as arranged in Article 2, and the right of self-defence, as arranged in Article 51 of the Charter of the United Nations, are accepted among the basic guidelines in international relations.

At the invitation of NATO's Centre of Excellence on Cyberdefence in Tallinn, Estonia, an independent "International Group of Experts" wrote "The Tallinn Manual on the International Law Applicable to Cyberwarfare," which states that "a state may exercise control over cyber infrastructure and activities within its sovereign territory" and points out that any attack against such an infrastructure is subject to jurisdiction.[32]

Despite the Manual, it is still open to discussion how to determine the critical threshold for an attack to be considered an armed attack to invoke Article 51 of the UN Charter. Since a cyberattack is not a conventional armed attack, it is also controversial whether a cyberattack can be considered as an armed attack. Yet a convincing

evaluation seems to be regarding the effect of the action. Just as bombs or missiles cause the destruction of human life and property, a suicide bomber can cause damage using his/her own body as a weapon. Similarly civil airliners were used as weapons during the attacks on the World Trade Center on 11 September 2011, resulting in mass-destruction. Since terrorists can use anything as a weapon, the concept of "armed attack" is better to be interpreted focusing on the effect of the assault, not on the process.

In this sense, as the world is not static, wide-scope interpretation is needed as regards the norms in international law. The same should apply to the concept of "weapon." Instead of depending on the availability of a tangible weapon, the resultant destruction through the use of any device should be taken into consideration. Karl Zemanek refers that "it is neither the designation of a device, nor its normal use, which make it a weapon, but the intent with which it is used and its effect."[33]

In Article 51 of the UN Charter covering the right of "self-defence," no criterion is specified regarding the agent of an armed attack, be it a state or a non-state actor. If a cyberattack is certain to have been performed by a state, then it is noteworthy that the state subject to the attack keeps the right of self-defence.

Cyberterrorism and NATO

After the 9/11 terrorist attacks, which have brought about a radical change in security policies around the world, cyber defence became part of NATO's political agenda at the Prague Summit in 2002, and since then has gained an increasing attention of NATO partners. Although NATO made a call to improve its "capabilities to defend against cyberattacks" through the Prague Capabilities Commitment, in the following years the Alliance opted for using passive protection measures as had been called for by the military side.[34]

During the Lisbon Summit of 19-20 November 2010, a new Strategic Concept was approved which cited cyberattacks as having the potential to reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. This is the first Strategic Concept which considers cyberattacks as a threat.[35] At the Lisbon Summit, the Heads of State tasked the North Atlantic Council to revise the first NATO Policy on Cyber Defence dated 2008, which had been approved following the cyberattacks against Estonia. Thus, the second NATO Policy on Cyberdefence was approved by the NATO Defence Ministers on 8 June 2011, packaged with an action plan for its implementation. The 2011 Policy focused "on the protection of NATO networks and cyberdefence requirements related to national networks that NATO relies upon to carry out its core tasks."[36] The document emphasised that any collective defence response by NATO will be subject to political decisions of the North Atlantic Council,

enabling the Council to maintain its flexibility in deciding whether a course of action will be taken or not.

The 2012 Chicago Summit Declaration[37] covered certain commitments, such as to bring all NATO bodies under centralised cyber protection, to further integrate cyber defence measures into Alliance structures and procedures, to identify and deliver national cyber defence capabilities that strengthen Alliance collaboration and interoperability, to engage with relevant partner nations on a case-by-case basis and with international organisations in order to address the cybersecurity threats and to improve common security.

The main controversial issue regarding collaboration within the Alliance is whether Article 5 of the North Atlantic Treaty, regarding the principle of collective defence, precisely covers cyberattacks or not. It still remains to be settled whether this Article would be invoked in case a member state comes under a cyberattack instead of a conventional assault and how the attacker country would be given response.

Yet another equally important issue for the Alliance is how to identify which attack is an act of war and how to detect the source of the attack. Since identities can be easily disguised in cyberspace, attributing attacks to specific perpetrators is not an easy task. The attacker may route the cyberattack through many different countries and IP addresses. If the attacker is misidentified, then a risk of an "accidental war" emerges.[38]

Turkey's Activities Regarding Cybersecurity

Turkey's leading player in the field of information security is the Cybersecurity Institute (SGE), operating under BİLGEM (Informatics and Information Security Research Centre) of TÜBİTAK (Scientific and Technological Research Council of Turkey). The institute was establishment in 1997 as "Network Security Group." After successfully completing several projects, it was renamed to "Information Systems Security Group," and in 2012 to "Cybersecurity Institute" (SGE). SGE provides information security consultancy to public institutions and organisations and the private sector. Some of the services it provides include information system security training, open source code solutions, responding to computer-based incidents and information system security testing. Among the finalised projects on regulations and action plans are: "e-Transformation Turkey Project," "Information Society Strategy and Action Plan," "National Security Council (MGK) Declaration," cybersecurity workshops and exercises, and "Council of Ministers Decision on the Execution, Management and Coordination of National Cybersecurity Activities."

In order to increase the national cybersecurity awareness, strengthen organisational capacities to deal with against cyberattacks, and improve the intra and inter-organisa-

tional coordination, Turkey began to conduct regular exercises. The first National Cybersecurity Exercise was carried out in the period 25-28 January 2011. After the exercise, Minister of Transportation Mr. Binali Yıldırım pointed the need for ceaseless effort to maintain cybersecurity stating that "the exercise was a success; however, we have no chance for a sense of peace as if we are secure. As information technologies advance, security threatening factors improve themselves as well."[39]

The second National Cybersecurity Exercise was conducted between 25 December 2012 and 11 January 2013. At a meeting during the exercise, Mr. Binali Yıldırım stated that "today's wars are waged with information technologies, not with cannons and rifles." He pointed out that "cyber threat will increase even more in the future and there are rifts between governments with respect to the awareness of this issue."[40]

A cyberdefence unit under the Turkish Armed Forces was established in 2012. The "General Staff Warfare and Cyberdefence Command" aims to protect its information network against cyberattacks. The unit operates in coordination with the Ministry of Transport, Maritime Affairs and Communications, TÜBİTAK and NATO in both national and international missions.

Pursuant to the Council of Ministers Decision on the "Execution, Management and Coordination of National Cybersecurity Activities" dated 12 October 2012, a Cybersecurity Council was established. It is chaired by the Minister of Transport, Maritime Affairs and Communications. The Cybersecurity Council was assigned the duty of preparing policies, strategies and action plans on ensuring cybersecurity at national level. Accordingly, a National Cybersecurity Strategy and an Action Plan[41] were prepared. These documents aim at creating an infrastructure towards achieving:

- cybersecurity of all services, processes and data—and the systems involved in provisioning of these—provided by the public organisations and agencies using information technologies;
- the cybersecurity of information systems of critical infrastructures; and
- minimisation of the effects of cybersecurity incidents.

All public organisations and agencies, natural and legal persons, are obliged to perform the duties assigned by the Cybersecurity Council in accordance with its policies, strategies and action plans and to comply with the procedures, principles and standards determined by the Council.

Members of the Cybersecurity Council are the undersecretaries of the Ministries of Foreign Affairs, the Interior, National Defence, and Transport, Maritime Affairs and Communications, the undersecretaries of Public Order and Security and the National Intelligence Organisation, the Chief of Communications, Electronics and Information Systems of the Turkish General Staff, the Chairman of Information and Communica-

tion Technologies Authority, the President of the Scientific and Technological Research Council, the President of the Financial Crimes Investigation Board, the President of Telecommunications and the top managers from the ministries and public organisations that are to be determined by the Minister of Transport, Maritime Affairs and Communications. The Council held its first meeting on 21 December 2012 when the document containing the National Cybersecurity Strategy and the 2013-2014 Action Plan was approved. The document was put into effect by Council of Ministers Decision 28683 and upon promulgation in the Official Gazette on 20 June 2013.[42]

The Action Plan consists of 29 actions and 95 sub-actions under seven main titles, scheduled to be concluded in the period of 2013-2014. In the Plan, responsible/ relevant public organisations and agencies are determined for each action and sub-action. One public organisation and agency is appointed responsible for each action, yet, that action can have more than one relevant organisation and agency. In case of an appointment of more than one relevant organisation for an action, then all the relevant organisations and agencies should act under the coordination of the responsible organisation or agency while working in parallel with each other. Pursuant to one of the actions stipulated in the plan, a National Cyberincident Response Centre (USOM) and Cyberincident Response Teams (SOME) have been established officially by a related notification issued on 11 November 2013 in the official gazette, although USOM had started functioning already in May 2013. The Secretariat General of the National Security Council is appointed as a relevant organisation for the 29th action of "Integrating national cybersecurity concepts into the national security context."

Examples of Cyberattacks from the World and Turkey

Examples from the World

September 11, 2001 was a milestone in raising worldwide awareness of cyber threats and transforming traditional threat perceptions.[43] The terrorist attacks on the World Trade Center and the Pentagon, displaying how cyber tools could be manipulated to generate such large-scale destruction, revealed even to the ordinary man that cyberspace has vulnerabilities as well as the capacity to help save time and labour. During this borderless attack, the terrorist group blocked the reception of the distress signals from the hijacked planes and disabled air radar systems.

A computer worm named "Stuxnet" targeting a nuclear facility in Iran in 2010 caused the damage of numerous nuclear enrichment centrifuges. "Stuxnet" has broken down the common but incorrect idea that "infection of a computer system by a computer virus may result in loss of files; yet if the data has been backed up, then the files can be restored." Stuxnet gained a valid reputation for targeting not only Internet-connected computer systems, but also closed computer systems.

Another outstanding example of a cyberattack was observed in 2007 against Estonia when websites of Estonian organisations and the country's Internet infrastructure were targeted after a Red Army war memorial in Tallinn had been removed. In Estonia, ranking 3rd in the world by intensity of Internet usage,[44] banking and finance systems almost came to collapse and the country was rescued from these attacks through the support by NATO.

"RedOctober" was a high-level cyberespionage campaign, which over five years, beginning from 2007, targeted computer networks of diplomatic and governmental agencies in addition to scientific research institutions, energy and aerospace companies in a wide range of countries, primarily in Eastern Europe and former Soviet republics – although many in Western Europe and North America were also included. "RedOctober," exploiting the vulnerabilities of Microsoft Word and Excel, sent spear-phishing e-mails with an attachment which was either an Excel or a Word document with enticing names, one of which was "Diplomatic Car for Sale.doc." The primary objective was to access confidential information, compromising the security of governments, corporations or other organisations. It was uncovered in early 2013 by experts from Russia's Kaspersky Lab.[45]

Examples from Turkey

In Turkey there are local websites operating against the national interests of the country. Generally, they are linked with separatist groups, aiming to disseminate propaganda and provide online training. Even if they are legally banned, some continue to operate through servers located in the United States and other Western countries (especially Germany, The Netherlands and France).

In June 2011, in a protest against the proposed internet filtering rules, planned to be put into action as of 22 August, the international hacker collective "Anonymous" (Anonymous describes itself as an "internet gathering" or a "hacker collective" rather than a "group") threatened to attack Turkey in a YouTube video. A Turkish manual regarding how the operation was to be executed and how the risk was to be minimised while attacking was also circulated on the Internet. The manual guided the common Internet user to download the necessary programmes to launch an attack and stay in contact with each other. The attacks of the collective mostly targeted the website of the Telecommunications Communication Presidency; however, thanks to the precautions taken, the website maintained functioning except for a short interruption.

In 2012, "Anonymous" again threatened Turkey over YouTube, announcing that they would start attacking Turkish government websites until Turkey recognises the alleged Armenian genocide. Thereafter, they performed attacks targeting the Ministries of the Interior, Foreign Affairs and Justice; yet the responses of the experts from the

Telecommunications Communication Presidency were successful enough to repel the attacks.

Final Remarks and Conclusion

In recent decades, along with the new technologies appearing at an unprecedented rate, new vulnerabilities, challenges and threats have emerged as well. It is vitally important to take efficient and timely measures against potential challenges and threats. Although current cybersecurity legislation of Turkey meets requirements in this field adequately, it would not be possible to achieve a complete legal cybersecurity framework, due to the high speed of technological developments and the ability of organised crime and terrorist groups to quickly and flexibly adapt themselves to such changes. Therefore, the central task is to develop and implement a comprehensive strategy covering all dimensions of cybersecurity, namely administrative, technical, legal, political, economic and social. The Cybersecurity Council provides coordination among public organs as envisaged by the existing National Cybersecurity Strategy and the 2013-2014 Action Plan; however, although the National Strategy stresses upon the requirement for coordination with the private sector, the Action Plan does not include any representative from the private sector with respect to implementation. In order to better address the cybersecurity of Turkey, it is particularly important to ensure an active participation of the private sector in the national efforts. On the other hand, producing legislation accordingly will also significantly contribute to cybersecurity in Turkey.

Despite the availability of related laws and regulations, a sufficient level of public awareness of cybersecurity has not yet been attained in Turkey. Hence, it is undeniably important that more books, reports and articles be published to better inform the public on cyber threats and challenges. Besides, broadcasting short movies, documentaries and public service announcements could facilitate attracting the attention of more people. Also, universities need to undertake responsibilities regarding the matter. In a research carried out in 2011, curricula of computer engineering departments of 20 universities of Turkey were investigated, revealing that seven universities had no courses at all on cybersecurity, nine universities had only one course, three universities had two courses and one university had three courses. Currently four universities (Bahçeşehir University, Gazi University, İstanbul Aydın University and Sakarya University) provide cybersecurity master's degree programmes. At the Middle East Technical University (METU) in Ankara, which has hosted various conferences on cybersecurity, a centre under the name of "Cyber Defence and Security Research Laboratory" (CyDeS) was established in April 2014. As per the National Cybersecurity Strategy and 2013-2014 Action Plan, universities are among the relevant organisations with respect to wider adoption of cybersecurity curricula in universities, edu-

cating academics in the study of cybersecurity (providing scholarship programmes), creating scholarship programmes for students who would like to specialise in cybersecurity, organising national and international cybersecurity events, promoting the usage of open source products and creating national products and solutions in the field of cybersecurity. In order to create awareness on the issue at early ages, it is quite significant that curricula of high and higher schools include elective courses on cybersecurity and technical high schools cover a cybersecurity programme besides programmes such as "Computer Technical Services," "Information Technologies," etc.

To ensure efficient cybersecurity, each and every person and institution capable of contributing to the cybersecurity of public organisations and agencies must be won. Such people and institutions, particularly public organisations and agencies, would benefit by training qualified cybersecurity personnel. In this regard, it is necessary to determine which personnel would get relevant theoretical and practical training. Furthermore, it is also important to allocate a sufficient budget for effectively combating cyberattacks.

It seems beneficial to switch from traditional protection mechanisms we are currently using, such as signature-based firewalls and anti-virus software, which are designed to mainly detect and protect against known threats, to behaviour-based security mechanisms, which aim at identifying a behaviour that is different than a normal one and blocking the attack, without a requirement of new rules and signature updates. On the other hand, cloud computing, which allows users to store and access data and programmes through remote servers over the Internet without the need for personal hard drives, is claimed to be more secure and cheaper. A test programme demonstrated that the US Department of Defence would save 30% on potential information technology by using the cloud network system.[46] Therefore, it would be beneficial for public organisations and agencies of Turkey to use two types of cloud computing systems, one of which ought to be a closed platform to ensure confidentiality of activities and records and the other – an open platform enabling connection to the whole Internet world-wide.[47]

One of the actions envisaged by the 2013-2014 Action Plan involves the establishment of emergency response teams, which are planned to conduct cyber crisis management. Although a National Cyberincident Response Centre (USOM) and Cyberincident Response Teams (SOME) were established officially and USOM started functioning, SOMEs still wait to be put into operation. SOMEs should be established as soon as possible and public organisations and agencies should prepare cyberincident response plans within the context of their own duties and responsibilities. It is important that the coordination and communication between the private sector of critical infrastructure and cyberincident response units be established through a network independent of the current internet system.

Providing countrywide secure Internet service is necessary for protection against cyberattacks, yet necessary arrangements should be made to meet the demands of users if they ask their Internet Service Providers (ISPs) for stronger protection. Relatedly, ISPs should better inform any of their users in case they detect that the user's computer has become a zombie computer, and even provide free anti-virus software to the victim customer.

In order to ensure cybersecurity, it is imperative that R&D efforts be intensified. This requires the support of both the government and the public sector. It is expected that such efforts would lead to the production of national software, which would help Turkey prevent potential risks and threats lurked in software of foreign origin, as well as to save national funds. Yet one of the most significant weaknesses in cybersecurity efforts in Turkey is observed in the field of R&D efforts, lacking an efficient coordination between public organisations and agencies and the private sector. Therefore, in order to overcome the weakness in question, necessary arrangements should be made to create an environment facilitating coordination between the public and private sectors with respect to technical support, training and R&D studies, as well as intelligence sharing.

In general, considering that responding to modern threats on one's own could not be really successful and combating such borderless threats is a collective endeavour, the need for international cooperation has become more urgent than ever. Therefore, international agreements are playing ever more important role in global security efforts. It is obvious that the same applies to cybersecurity. The rapid development in communication technologies has removed the national boundaries, increasing and gradually deepening the interaction between countries. A malware causing harm and destruction in one country may easily spread to other countries and threaten national security. In order to prevent countries from this dark side of globalisation and mitigate the spread of malware, international cooperation is of great importance. Thus, Turkey needs to continue her efforts to conclude international agreements in this context. These agreements may cover areas such as cyberdefence cooperation, cyber non-aggression, prevention of cybercrime, mutual legal assistance in criminal matters and extradition, training, scientific-technological cooperation and cyber intelligence sharing.

With the Internet becoming part of our lives, the concept of "cyberterrorism" has emerged as a buzzword, used widely in both national and international arenas. Technologies have become so common all around the world that organised crime and terrorist organisations can easily exploit the opportunities they provide.

The terrorist attacks on the twin towers of New York's World Trade Center on 11 September 2001 changed radically global counterterrorism efforts. Countries have

deemed it necessary to reconsider the security of their critical infrastructures and their cybersecurity measures as well as their traditional defence systems.

Attacks in the cyber domain evolve so rapidly that legal arrangements cannot cope with evolving security requirements of an individual and a nation, and need to be frequently updated. Turkey, too, has made important attempts at combating cyber threats and put various resolutions and action plans into effect. Yet, in order to strengthen the cybersecurity efforts, it is necessary to further the international cooperation as well as the cooperation between the public bodies and the private sector.

Notes:

[1] Nazife Baykal, "Bilgi Teknolojisinin, Ulusal Güvenlik ve Ulusal Güvenlik Startejisi ile İlgili Boyutu" (Information Technology in relation to National Security and the National Security Strategy), International Conference on "New Dimensions of Security and International Organizations," organised by the Turkish Armed Forces, Istanbul, 31 May – 2 June 2007.

[2] ICT Facts and Figures, "The World in 2015," accessed on 27 June 2015, available at http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

[3] Walter Laqueur, "Postmodern Terrorism: New Rules for an Old Game," *Foreign Affairs*, September/October 1996, accessed on 9 July 2015, https://www.foreignaffairs.com/articles/1996-09-01/postmodern-terrorism-new-rules-old-game.

[4] ISI was a non-profit research organisation, dedicated to the study of man-made disasters. It was closed in 2000.

[5] Barry Collin, "The Future of CyberTerrorism," *Crime & Justice International* 13, no. 2 (March 1997), accessed on 9 July 2015, available at http://www.cjimagazine.com/archives/cji4c18.html?id=415.

[6] Mark M. Pollitt, "Cyberterrorism — Fact or Fancy?" *Computer Fraud & Security* 2 February 1998): 8-10, http://dx.doi.org/10.1016/S1361-3723(00)87009-8.

[7] Nihat Ali Özcan, "Küreselleşme Bağlamında Terörizmle Mücadele" (Counter-Terrorism within the Context of Globalization), *Birinci Uluslararası Sempozyum Bildirileri: Küreselleşme ve Uluslararası Güvenlik (The Proceedings of the First International Symposium on Globalization and International Security)*, SAREM, Ankara, 2003, 3.

[8] Mesut Hakkı Caşın, *Uluslararası Terörizm (International Terrorism)* (İstanbul: Nobel, 2008), 459.

[9] Richard A. Clarke and Robert K. Knake, *Siber Savaş-Ulusal Güvenliğe Yönelik Yeni Tehdit (Cyber War: The Next Threat to National Security and What to Do About It)*, Trans.Murat Erduran (İstanbul: İstabul Kültür University, 2011), 23-24.

[10] The US banks' websites were blocked in 2012 for several weeks due to cyberattacks, which caused loss of millions of dollars.

[11] Debarati Halder and K. Jaishankar, *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations* (Information Science Reference, 2011), 15.

[12] Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?" *Studies in Conflict & Terrorism* 28, no. 2 (2005): 129-149, accessed on 7 June 2015, http:/dx.doi.org/10.1080/10576100590905110.

[13] United Nations Office on Drugs and Crime, "Transnational Organized Crime: The Globalized Illegal Economy," accessed on 3 June 2014, www.unodc.org/toc/en/crimes/organized-crime.html.

[14] Symantec Corporation, *Symantec Internet Security Threat Report/Trends for January – June 07*, vol. 12 (September 2007), accessed on 9 July 2015, available at http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf.

[15] Ponemon Institute, "2013 Cost of Cyber Crime Study: United States," Research Report (2013), 2, accessed on 2 June 2014, available at http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf.

[16] Howard F. Lipson, "*Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*," Special Report CMU/SEI-2002-SR-009 (Carnegie Mellon University Software Engineering Institute, 2002), 10, accessed on 9 July 2015, http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5831.

[17] Caşın, 452.

[18] Ibid.

[19] Ibid, 453.

[20] Clarke and Knake, 75.

[21] 95% of US critical infrastructure is connected to the electrical infrastructure. Therefore, cyberterrorism has been declared as the greatest threat.

[22] Hasan Çiftçi, *Her Yönüyle Siber Savaş* (Ankara: TÜBİTAK, 2013), 25.

[23] Ibid, 43.

[24] UK Cabinet Office, *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space*, June 2009, accessed on 8 July 2015, www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf.

[25] UK Parliament, "Written Answers," Questions by Lord Patten on Cybersecurity, 3 December 2009, accessed on 7 July 2015, available at www.publications.parliament.uk/pa/ld200910/ldhansrd/text/91203w0001.htm; SearchSecurity.co.UK, "Office of Cyber Security and Information Assurance (OCSIA)," accessed on 7 July 2015, available at http://searchsecurity.techtarget.co.uk/definition/Office-of-Cyber-Security-and-Information-Assurance-OCSIA.

[26] Houses of Parliament Parliamentary Office of Science and Technology, "Cyber Security in the UK," Postnote no. 389, September 2011, accessed on 7 July 2015, available at http://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-UK.pdf.

[27] UK Cabinet Office, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, October 2010, accessed on 7 July 2015, available at www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf.

[28] UK Cabinet Office, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, October 2010, accessed on 7 July 2015, available at www.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf.

[29] UK Cabinet Office, *Update on the National Cyber Security Programme*, HC 626 Session 2014-15, 10 September 2014, accessed on 6 July 2015, available at www.nao.org.uk/wp-content/uploads/2015/09/Update- on-the-National-Cyber-Security-Programme.pdf.

[30] *The French White Paper on Defence and National Security* (2008), accessed on 9 July 2015, available at www.cfr.org/content/publications/attachments/Dossier_de_presse_LBlanc_DSN_en_anglais.pdf.

[31] *French White Paper on Defence and National Security 2013*, accessed on 9 July 2015, available at http://www.livreblancdefenseetsecurite.gouv.fr/pdf/the_white_paper_defence_2013.pdf.

[32] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013), 25, accessed on 4 July 2015, available at www.knowledgecommons.in/wp-content/uploads/2014/03/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf.

[33] Karl Zemanek, "Armed Attack," *Max Planck Encylopedia of Public International Law*, Encyclopedia Entries, last updated October 2013, accessed on 9 July 2015, available at http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e241?rskey=8QR192&result=2&prd=EPIL.

[34] Olaf Theiler, "New Threats: The Cyber Dimension," *NATO Review Magazine*, accessed on 8 July 2015, available at http://www.nato.int/docu/review/2011/11-september/cyber-threads/en/index.htm.

[35] NATO's Strategic Concept of 1999 discussed the issue as follows: "State and non-state adversaries may try to exploit the Alliance's growing reliance on information systems through information operations designed to disrupt such systems. They may attempt to use strategies of this kind to counter NATO's superiority in traditional weaponry."

[36] *Defending the Networks: NATO Policy on Cyber Defence* (2011), accessed on 8 July 2015, available at http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf.

[37] North Atlantic Treaty Organization, "Chicago Summit Declaration," 20 May 2012, last updated on 1 August 2012, accessed on 5 July 2015, available at www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en.

[38] Two guided missiles were sent from the US ship "Saratoga" to a Turkish battleship in NATO exercises in 1992 and 5 Turkish soldiers were martyred.

[39] "41 Kuruma Siber Savaş ilan Edildi: Siber Savaş Alarmı!" (War Declared on 41 Agencies: Alarm Bell for Cyber War!), *BT Haber.com*, 30 January 2011, accessed on 3 June 2014, available in Turkish at https://www.bthaber.com/41-kuruma-siber-savas-ilan-edildi-siber-savas-alarmi.

[40] The Scientific and Technological Research Council of Turkey/TÜBİTAK; "2. Ulusal Siber Güvenlik Tatbikatı Başarıyla Tamamlandı" (Second National Cyber Security Exercise Proves Success), 1 January 2013, accessed on 3 June 2014, available at www.tubitak.gov.tr/tr/haber/2-ulusal-siber-guvenlik-tatbikati-basariyla-tamamlandi.

[41] Republic of Turkey Ministry of Transport, Maritime Affairs and Communications, *National Cyber Security Strategy and 2013-2014 Action Plan*, accessed on 7 July 2015, http://www.udhb.gov.tr/doc/siberg/ActionPlan2013-2014.pdf.

[42] Official Gazette, 20 June 2013, accessed on 25 June 2014, available in Turkish at http://www.resmigazete.gov.tr/eskiler/2013/06/20130620.pdf.

[43] Theiler, "New Threats: The Cyber-Dimension."

[44] "e-Estonia" is the term commonly used to describe Estonia's emergence as one of the most advanced e-societies in the world.

[45] Kaspersky Lab, "Kaspersky Lab Identifies Operation 'Red October," an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide," 14 January 2013, accessed on 7 July 2015, available at www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide; "Red October Analysis Reveals Complex, Two-Stage Attack," *InfoSecurity*, 17 January 2013, accessed on 7 July 2015, available at www.infosecurity-magazine.com/news/red-october-analysis-reveals-complex-two-stage/; Dan Raywood, "Red October Espionage Campaign Targets Governments and Organisations," *SC Magazine*, 14 January 2013, accessed on 7 July 2015, available at http://www.scmagazineuk.com/red-october-espionage-campaign-targets-governments-and-organisations/article/275902/.

[46] Gerry J. Gilmore, "DOD, Industry Address 'Intense Challenge' of Cyber Security," *US Department of Defence*, 7 November 2011, accessed on 6 June 2014, available at http://www.defense.gov/news/newsarticle.aspx?id=65988.

[47] Çiftçi, 389.

Ata ATALAY, Ph.D., received his License Degree from the Department of City and Regional Planning at the Middle East Technical University (METU) in Ankara, Turkey (1979). He attained his Master's Degree in Environmental Design at METU (1983) and his Ph.D. Degree at Ankara University (2008). In 1989-1990, he conducted research studies at the Massachusetts Institute of Technology and Harvard University. He started his career in 1979 as an expert at the Undersecretariat of Environment under the Prime Minister. Then he successively worked as an Expert at the State Planning Organisation, Advisor at the Secretariat-General of the National Security Council, Project Manager at UNICEF Turkey, expert at the Directorate General of Foreign Economic Relations under the State Planning Organisation. Since 2002 he has been working at the Secretariat General of the National Security Council of Turkey. First he served as an advisor at the Department of National Security Policy, then as a Group Head at the Department of Research and Evaluation and since 2014 he has been the Deputy Head of the Department of Research and Evaluation. He is fluent in English and intermediate in German. *E-mail*: aatalay56@yahoo.com

Gurur SANCI graduated from the Department of Political Science and Public Administration at the Middle East Technical University (METU) in Ankara, Turkey (2012). In 2013-2014 he worked as an Assistant Expert at the Directorate General of Press and Information under the Office of Prime Minister. He has been working as an Assistant Expert at the Secretariat General of the National Security Council. He is a Graduate Student of the Master of Arts Programme in African Studies at Ankara University, fluent in English.